-Technical Whitepaper -

high technology for virtual private network solutions

msm net ingenieurbüro meissner

Am Porstendorferweg 4
D 07570 Niederpöllnitz - Germany

Table of contents

1. Preface

The current „technical whitepaper“ is addressed to technically experienced decision-makers as well as system administrators. It presents in a short and clear way the important technical characteristics.
On the basis of these tables a fast evaluation of possible advanced variants and system integrations can take place.
We offer an extented dialogue to every reader interested in it. In the following paragraph you can inform yourself on the enormous scaling capabilities.

2. General technical potential

Using the VPN solutions of „msm net ingenieurbüro meissner“ means that any VPN-network structures can be realized. With the use of the internet classic star-type and meshed networks as well as combinations can be realized. The realization can be carried out either with static and/or dynamic IP-addresses.

Starting out from these facts, VPN can be realized both in the stationary and in the mobile area. All and any combinations can be administered via existing administration tools from a central place.

As a rule, there are very different hardware standards necessary for the technical realization. The technical solutions of „msm net ingenieurbüro meissner“ open up an enormous range.

According to technical requirements, rather simple (without hard disc, CD-ROM and FD) but also very demanding solutions (multiprocessor design systems...) can result from this.

Through our modular concept, the technical access to the internet as a medium of transport can be arranged in a very flexible way, too.

It goes without saying that each VPN router is equipped with a firewall.

3. Technical data of VPN software

Category	Details
Operationsystem	Linux
System hardware	PC components, scaling hardware variants Minimalsolution: without hartddisc, CDROM and FD, with essentials interfaces
Max. VPN connection	unlimited
Authentification	-MD5 - SHA - SHA2-256 - SAH2-512
Cryptografy operations	-3DES - AES 128 - AES 192 - AES 256 - Blowfish 128 - CAST 128 - Twofish - Serpent
DH group bitlenght	-768 -1024 - 2048 - 3072 - 4096 - 6144 - 8192

VPN connection types	- IPSEC - PPTP - L2TP over IPSEC
Tunnel types	- GRE - IP over IP
IP address types	- IPv4 und IPv6 - static - dynamic
Autom. disconnetion	configurable
Autom. rekeying	configurable
Certificat administration	- ROOT- and SUB-CA certificates - user certificates - CRL, OSCP - cryptosmartcard application
Authentification methodes	- X509 certifikates (too cryptosmartcard) - PSK
Logfiles	- configurable per e-mail - central logfile saving with automatic controling
System redundancy	Redundancy control for media and peers addressing (OSPF, RIP, DynDNS, ...)
Max. datatroughput	unlimited, dependent from hardware

4. Basis RFCs of VPN software

Overview RFCs
2401 Security Architecture for the Internet Protocol
2411 IP Security Document Roadmap

Basic protocols
2402 IP Authentication Header
2406 IP Encapsulating Security Payload (ESP)

Key management
2367 PF_KEY Key Management API, Version 2
2407 The Internet IP Security Domain of Interpretation for ISAKMP
2408 Internet Security Association and Key Management Protocol (ISAKMP)
2409 The Internet Key Exchange (IKE)
2412 The OAKLEY Key Determination Protocol
2528 Internet X.509 Public Key Infrastructure

Details of various things used
2085 HMAC-MD5 IP Authentication with Replay Prevention
2104 HMAC: Keyed-Hashing for Message Authentication
2202 Test Cases for HMAC-MD5 and HMAC-SHA-1
2207 RSVP Extensions for IPSEC Data Flows
2403 The Use of HMAC-MD5-96 within ESP and AH
2404 The Use of HMAC-SHA-1-96 within ESP and AH
2405 The ESP DES-CBC Cipher Algorithm With Explicit IV
2410 The NULL Encryption Algorithm and Its Use With IPsec
2451 The ESP CBC-Mode Cipher Algorithms
2521 ICMP Security Failures Messages

Older RFCs which may be referenced
1321 The MD5 Message-Digest Algorithm
1828 IP Authentication using Keyed MD5
1829 The ESP DES-CBC Transform
1851 The ESP Triple DES Transform
1852 IP Authentication using Keyed SHA

Related RFCs
1750 Randomness Recommendations for Security
1918 Address Allocation for Private Internets
1984 IAB and IESG Statement on Cryptographic Technology and the Internet
2144 The CAST-128 Encryption Algorithm

5. Project oriented problem solutions

For the planning and realization of a VPN, all matters of technial significance of existing networks as well as their technical connection to the internet and the mobile communication of the external service have to be taken into consideration.

For this reason it is especially important that first of all an ACTUAL-analysis is carried out of all parts to be integrated. Starting from this ACTUAL-analysis, a clear object definition can be made including all necessary measures and requirements.

We offer you the following services for the realization of your VPN:

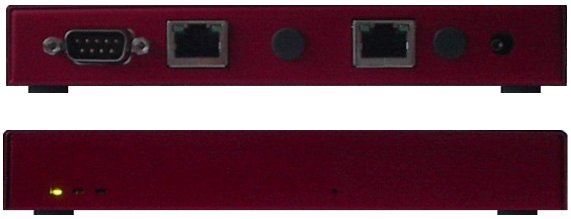
Consulting, planning and projection services for the establishment of VPN within the international and national environment

- Working out of an operating plan for VPN-networks
- Working out of a quantity structure for the definition of hardware requirements
- Installation, configuration, and putting into operation of hardware and software and components of the VPN
- Supervising and evaluation of protocol files
- Regular assurance tests
- Remote as well as local service and maintenance
- Instruction and training of local administrators

Using our products makes it possible to interlink any number of local networks and external staff in one VPN via the internet.

For further information we will be at your disposal at any time.

6. VPN Router Variants

Mini-VPN-Router	
	The mini VPN routers come in a very stable aluminum case with the dimensions (WxDxH) 15,5 cm x 15,5 cm x 2,5 cm. Interfaces: 2 x 10/100 Mbit Datathroughput: up to 8Mbit with 3DES-MD5-2048

Midi-VPN-Router	
	Midi-VPN-Router variants: standalone or 19“ (with 22 oder 45 cm Depth) possible Interfaces: 2x 10/100 Mbit, opt. and ADSL, ISDN Datathroughput: up to 35 Mbit with 3DES-MD5-2048

Maxi-VPN-Router	
	Maxi-VPN-Router variants: Servercases or 19“ (1 he with 45 cm Depth) possible Interfaces: 2x 10/100/1000 Mbit Datathroughput: over 200 Mbit with 3DES-MD5-2048

Midi-HC-VPN-Router	
	Midi-HC-VPN-Router use by AES-encryption and SHA-authentification the Padlockengine from the VIA C7 processor. possible Interfaces: 2x 10/100/1000 Mbit, TP, SC, ST Datathroughput: ca. 11 Mbyte with AES128-SHA128-2048 in a 100 Mbit network. ca. 25 Mbyte with AES128-SHA128-2048 in a 1000 Mbit network.

Maxi-HC-VPN-Router	
	Maxi-HC-VPN-Router use by AES-encryption and SHA-authentification the Padlockengine from the VIA C7 processor. possible Interfaces: 2x 10/100/1000 Mbit, TP, SC, ST Datathroughput: ca. 11 Mbyte with AES128-SHA128-2048 in a 100 Mbit network. ca. 110 Mbyte with AES128-SHA128-2048 in a 1000 Mbit network.

Special interface requests can be realized on demand.

Optional Equipment	Mini-Router	Midi-Router	Maxi-Router
Cryptosmartcart Application	✔	✔	✔
Hardware Cryptografy (only devices without VIA C7 processor)	✔	✔	✔

Through the use of hardware cryptography it is possible to realize very high safety requirements and increase performances at the same time.

7. Service and maintenance work

„msm net ingenieurbüro meissner“ offers an extensive service and maintenance work for all of his products.
These services and maintenance work are being phased according to call- and guaranteed error-correction times and are offered within the framework of maintenance contracts.Training, instruction, and consultations

8. Training, instruction, and consultations

Qualified staff members are an essential precondition for an effective reaching of your business objectives. Therefore we would like to instruct your staff on subjects such as follows:

- VPN administration,
- External work and service networks,
- e-mail-applications,
- System- and network administration,
- Internet and procurement of information
- Data security.

9. Contact data

Address

msm net ingenieurbüro meissner

Am Porstendorferweg 4

D - 07570 Niederpöllnitz - Germany

Communication

Telefon : +49 (0) 36607 60567

Fax : +49 (0) 36607 60577

Handy: +49 (0) 0170 24190 25

e-mail : service@msm-net.de

Internet : www.msm-net.de